Exhibit G

RIDGEVIEW MEDICAL CENTER AND CLINICS **#3508**

SUBJECT: DATA CLASSIFICATION POLICY

ORIGINATING DEPT: Information Technology **DISTRIBUTION DEPTS:** All

ACCREDITATION/REGULATORY STANDARDS:

Original Date: 12/12 **Revision Dates:** **Reviewed Dates:**	**APPROVAL:** Administration: ______________________ Director: ______________________

PURPOSE:

The purpose of the Ridgeview Medical Center Data Classification Policy is to provide a system for protecting information that is critical to the organization, and its customers. In order to provide more appropriate levels of protection to the information assets entrusted to Ridgeview Medical Center, data must be classified according to the risks associated with its storage, processing, and transmission. Consistent use of this data classification policy will facilitate more efficient business activities and lower the costs of ensuring adequate information security.

Audience

The Ridgeview Medical Center Data Classification Policy applies equally to any individual, or process that interacts with Ridgeview Medical Center Information Resources in any tangible manner. All personnel who may come in contact with "Confidential" information are expected to familiarize themselves with this Data Classification Policy and consistently use it.

POLICY:

Responsibility for Data Management

Data is a critical asset of Ridgeview Medical Center, its business partners, and its patients. All individuals employed by Ridgeview Medical Center have the responsibility to protect the Confidentiality, Integrity, and Availability of the data generated, accessed, modified, transmitted, stored and/or used by Ridgeview Medical Center, irrespective of the medium on which the data resides and regardless of format (i.e. electronic, paper or other physical form).

Data User -

The Data User is a person, organization or entity that interacts with data for the purpose of performing an authorized task. A Data User is responsible for using data in a manner that is consistent with the purpose intended and in compliance with policy.

Data Owner -

The Data Owner is normally the person responsible for, or dependent upon the business process associated with an information asset. The Data Owner is knowledgeable about how the information is acquired, transmitted, stored, deleted, and otherwise processed.

- The Data Owner determines the appropriate value and classification of information generated by the owner or department;
- The Data Owner must communicate the information classification when the information is released outside of the department and/or Ridgeview Medical Center;
- The Data Owner controls access to his/her information and must be consulted when access is extended or modified; and

- The Data Owner must communicate the information classification to the Data Custodian so that the Data Custodian may provide the appropriate levels of protection.

Data Custodian -

- The Data Custodian maintains the protection of data according to the information classification associated to it by the Data Owner.
- The Data Custodian role is delegated by the Data Owner and is usually Information Technology personnel.

Data Classifications

Data owned, used, created or maintained by Ridgeview Medical Center is classified into one of the following three categories:

- Public
- Internal
- Confidential

Public Data -

Public data is information that may or must be open to the general public. It is defined as information with no existing local, national, or international legal restrictions on access or usage. Public data, while subject to Ridgeview Medical Center disclosure rules, is available to all Ridgeview Medical Center employees and all individuals or entities external to the corporation.

Examples of Public Data include:

- Publicly posted press releases
- Publicly available marketing materials
- Publicly posted job announcements

Disclosure of public data must not violate any pre-existing, signed non-disclosure agreements.

Internal Data -

Internal Data is information that must be guarded due to proprietary, ethical, or privacy considerations and must be protected from unauthorized access, modification, transmission, storage or other use. This classification applies even though there may not be a civil statute requiring this protection. Internal Data is information that is restricted to personnel designated by Ridgeview Medical Center, who have a legitimate business purpose for accessing such data.

Examples of Internal Data include:

- Employment data
- Business partner information where no more restrictive confidentiality agreement exists
- Internal directories and organization charts
- Planning documents
- Contracts

Internal Data:

- Must be protected to prevent loss, theft, unauthorized access and/or unauthorized disclosure
- Must be protected by a confidentiality agreement before access is allowed
- Must be stored in a closed container (i.e. file cabinet, closed office, or department where physical controls are in place to prevent disclosure) when not in use.

- Must be destroyed when no longer needed subject to the Ridgeview Medical Center Policy #3509 - *Data Retention*. Destruction may be accomplished by:
  - "Hard Copy" materials must be destroyed by shredding or another approved process which destroys the data beyond either recognition or reconstruction as per the data destruction and re-use standard. See Policy #3513 - *Media Reuse and Disposal* for more information.
  - Electronic storage media shall be sanitized appropriately by overwriting or degaussing prior to disposal as per the data destruction and re-use standard. See Policy #3513 - *Media Reuse and Disposal* for more information.
- Is the "default" classification level if one has not been explicitly defined.

Confidential Data -

Confidential Data is information protected by statutes, regulations, Ridgeview Medical Center policies or contractual language. Data Owners may also designate data as Confidential. All RMC data is considered confidential unless a media release process initiated.

Confidential Data is sensitive in nature, and access is restricted. Disclosure is limited to individuals on a "need-to-know" basis only.

Disclosure to parties outside of Ridgeview Medical Center must be authorized by executive management, approved by the Director of Management Information Services and/or General Counsel, or covered by a binding confidentiality agreement.

Examples of Confidential Data include:

- Protected Health Information ("PHI")/Medical records
- Financial information, including credit card and account numbers
- Social Security Numbers
- Personnel and/or payroll records
- Any data identified by government regulation to be treated as confidential, or sealed by order of a court of competent jurisdiction
- Any data belonging to an Ridgeview Medical Center customer that may contain personally identifiable information

Confidential Data:

- When stored in an electronic format must be protected with a minimum level of authentication to include strong passwords, wherever possible.
- A Mobile Device Management process manages Ridgeview data on mobile devices.
- Must be stored in a locked drawer, room, or area where access is controlled by a guard, cipher lock, and/or card reader, or that otherwise has sufficient physical access control measures to afford adequate protection and prevent unauthorized access by members of the public, visitors, or other persons without a need-to-know.
- Must be encrypted with strong encryption when transferred electronically to any entity outside of Ridgeview Medical Center.
- When sent via fax, must be sent only to a previously established and used address or one that has been verified as using a secured location.
- Must not be posted on any public website.
- Consistent with its respect for patients' privacy and confidentiality, confidential data incudes; photographs, videos or audio records of patients and/or staff.
- Must be destroyed when no longer needed subject to the Ridgeview Medical Center MIS Policy #3509 - *Data Retention*.

Destruction may be accomplished by:

- "Hard Copy" materials must be destroyed by shredding or another approved process that destroys the data beyond either recognition or reconstruction as per the data destruction and re-use standard. See Policy #3513 - *Media Reuse and Disposal* for more information.
- Electronic storage media that will be re-used must be overwritten according to the data destruction and re-use standard. See Policy #3513 - *Media Reuse and Disposal* for more information.
- Electronic storage media that will not be re-used must be physically destroyed according to the data destruction and re-use standard. See Policy #3513 - *Media Reuse and Disposal* for more information.
- Deleting files or formatting the media is NOT an acceptable method of destroying Confidential Data.

The Ridgeview Medical Center Director of Management Information Services must be notified in a timely manner if data classified as Confidential is lost, disclosed to unauthorized parties or is suspected of being lost or disclosed to unauthorized parties, or if any unauthorized use of Ridgeview Medical Center information systems has taken place or is suspected of taking place.

WAIVERS:

Waivers from certain policy provisions may be sought following the process outlined in the Ridgeview Medical Center Policy #3511 - *Enterprise Information Security Governance*.

ENFORCEMENT:

Any user found to have violated this policy may be subject to disciplinary action, up to and including termination of employment.

Any vendor, consultant, or contractor found to have violated this policy may be subject to sanctions up to and including removal of access rights and termination of contract(s).

VERSION HISTORY OF SOURCE DOCUMENT: Ridgeview Medical Center Information Security Policy Manual

Version Number	Date	Reason/Comments
V1.00	December, 2012	Document Origination
V2.00	May, 2014	Full review with IT Steering Committee
V3.00	August, 2015	Reviewed with Security Committee
	6/16	Finalized, assigned policy number, on RidgeNet. Previous documentation not archived.